



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY-DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/740,376      | 12/19/2000  | Chin-Long Chen       | POU920000124US1     | 3152             |

7590

07/22/2004

Lawrence D. Cutter, Attorney  
IBM Corporation  
Intellectual Property Law Dept.  
2455 South Rd., M/S P386  
Poughkeepsie, NY 12601

|          |
|----------|
| EXAMINER |
|----------|

HO, THOMAS M

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 07/22/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

4

## Office Action Summary

Application No.

09/740,376

Applicant(s)

CHEN ET AL.

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. **Claims 1 is pending**

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by “Applied Cryptography” Menezes et al.

In reference to claim 1:

Menezes(Section 14.32-14.41) discloses a method for checksum generation and utilization, in an apparatus for performing modulo N multiplication of integers A and B in which said modulo multiplication is carried out in k bit wide portions of the factors A and B which are representable and as

$$\sum (A_i R^i) \text{ For } I=0 \text{ to } M-1, \text{ and } \sum \text{ of } (B_i R^i) \text{ For } I=0 \text{ to } M-1$$

where R equals  $2^k$  and where N is representable as  $\sum \text{For } I=0 \text{ to } M-1, \text{ of } N_i R^i$ , said

method comprising the steps:

Art Unit: 2134

- Operating said multiplication apparatus over a plurality of cycles so as to produce, at each cycle  $I$ , the values  $Z_i$  and  $Y_i$  in accordance with a two phase modular multiplication method which does not require division operation., where Montgomery's Modular Multiplication Algorithm discloses a two phase method without requiring division, where the two phases are step 2.1 and 2.2 of 14.36, where  $A$  is  $Z_i$  and  $u_i$  is the values of  $Y_i$ .
- Accumulating, over said cycles, sums modulo( $R-1$ ) of the values  $A_i$ ,  $B_i$ ,  $N_i$ , and  $Z_i$ , where  $A$  of 14.36 is  $Z_i$ ,  $X$  and  $Y$  of 14.36 is  $A_i$  and  $B_i$ , and  $m_i$  is  $N_i$ , where the values are accumulated over the cycles of the for loop through their individual representations. Ex.  $M = (m_{n-1} \dots m_1 m_0)$
- Comparing the sum of the  $Z_i$  values with the sum of two products, the first product being the product of the sums of the  $A_i$  and  $B_i$  terms, and the second product being the product of the sums of the  $N_i$  and  $Y_i$  terms, where the sum of the  $Z_i$  values ( $A$  of 14.36) are compared using the sums of two products(  $x_i y$  and  $u_i m$ ) from 2.2 of 14.36.

The Examiner notes that it is well known it is well known in the art the Binary numbers in computers are a base two system, and where a base  $N$  system of numbers if a system where a number contains digitals  $A_i$  to  $A_0$

such that the quantity expressed by  $A_i A_{(i-1)} A_{(i-2)} \dots A_1 A_0$  is equivalent to

$$(A_i * N^i) + (A_{i-1} * N^{(i-1)}) + \dots + (A_2 * N^2) + (A_1 * N^1) + (A_0 * N^0) \text{ which is the}$$

quantity expressed by

Art Unit: 2134

$\sum$  For  $I=0$  to  $M-1$ , of  $A_i R^i$  where  $R$  equals  $2^k$ . Therefore, the factors  $A$  and  $B$  merely disclose properties characteristic of numbers represented in base 2.

### *Conclusion*


4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US patent 6,182,104 discloses a method of modulo multiplication that reveals some aspects/variations of the Montgomery multiplication method.
- "Analyzing and Comparing Montgomery Multiplication Algorithms" by Koc et al. discloses a number of variations on the Montgomery multiplication method, each of which avoid the use of division.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Application/Control Number: 09/740,376  
Art Unit: 2134

Page 5

TMH

July 9<sup>th</sup> 2003